



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/779,862

02/18/2004

Roberg Skog

4147-64

6213

23117 7590 05/02/2008
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT

PAPER NUMBER

2134

MAIL DATE

DELIVERY MODE

05/02/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/779,862	Applicant(s) SKOG ET AL.	
	Examiner MICHAEL J. SIMITOSKI	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 February 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8, 12-16 and 19-21 is/are rejected.
- 7) ☒ Claim(s) 9-11, 17 and 18 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The response of 2/21/2008 was received and considered.
2. Claims 1-21 are pending.

Oath/Declaration

3. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:

Inventor Skog has listed first name “Roberg”, where the specification lists “Robert”.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification does not disclose “circuitry” or “interface” such as is presented in claims 12-21.

Response to Arguments

5. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection. However, several comments on the new rejections are made below in an effort to further prosecution.

6. Applicant's amendment to claim 1 recites "said device-type associated commitment being a commitment for devices of a particular device-type regarding what capability the devices support". In terms of the cited IPsec, not only is the Internet Protocol (IP) header used, but a signature in a second header is included for integrity in each IPsec message between two participants. One of the data fields of the IP header (over which the IPsec authentication header includes a digital signature), is the IP version number. In light of this claim language, the Stallings reference discloses a capability (the commitment to the capability to interpret IPv4 or IPv6 protocols) and a signature over that commitment. What Stallings (IPsec) does not disclose, is determining the device's capability based on this version number and creating a second, comparison, signature based on tamper-resistant information associated with a determined device-type. The IPsec authentication header is merely used to examine the data received, create a second signature over that data and determine if the signatures match. The step of creating a signature using tamper-resistant information associated with a device-type that was determined using the first header is not disclosed.

7. OMA is cited for teaching that a capability (device type identifier) can be included in an HTTP request message. Stallings is further cited for teaching the well known SSL (or HTTPS) protocol, such that a signature is created over a standard HTTP packet.

8. In light of the new reference combination cited against previously allowed claims 3, 14 & 20, this rejection is made **NON-FINAL**.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1, 4-6, 8, 16 & 21 are rejected under 35 U.S.C. 102(b) as being anticipated by IP Security, described in Network Security Essentials, Applications and Standards by **Stallings**.

Regarding claim 1, Stallings discloses providing, in a first device connected to said communication system (Sender/host, p. 172, §Anti-replay service, ¶2 & p. 174, Fig. 6.5, computer on right side communicating with server on the left side), first header information of a communication message (IP header, p. 175, Fig. 6.6(c), IPv4), said first header information being related with a device-type associated commitment (IP header includes version number supported, p. 197, §IPv4), said device-type associated commitment being a commitment for devices of a particular device-type regarding what capability the devices support (support for IPv4, p. 197, §IPv4), tamper-resistantly (HMAC, p. 173) creating a first signature in said first device (sender) based on at least tamper-resistant device-type information of said first device (MAC is calculated over immutable header fields, p. 173, §Integrity Check Value, ¶3+, which include the version), providing, in said first device (sender), second header information (authentication header) of said communication message (p. 175, Fig. 6.6(c)), communicating said communication message to a second device connected to said communication system (packet is routed to destination, p. 179, #2) and authenticating said first header information by verifying said first signature after said communicating step (authentication header authenticates the inner IP packet, p. 169, #3, p. 171, ¶1 & destination processes headers, p. 180, #3).

Regarding claim 4, Stallings discloses wherein said first device (sender) is a user terminal (end user, p. 163, §Applications of IPSec, “Secure remote access ...”). See also p. 174, Fig. 6.5 for another example of this.

Regarding claim 5, Stallings discloses wherein said second device is a server (ISP, p. 163, §Applications of IPSec, “Secure remote access ...”). See also p. 174, Fig. 6.5 for another example of this.

Regarding claim 6, Stallings discloses wherein said device-type specific information comprises a definition of an algorithm according to which said signature is to be created (the entities in IPSec communication use HMAC-MD5-96 or HMAC-SHA-1-96 and as such, the signature is created using one of these definitions, p. 173, §Integrity Check Value).

Regarding claim 8, Stallings discloses wherein said step of creating a signature is additionally based on at least one item in the group of: time, date and header information (based partly on header information, p. 173, last 2 paragraphs).

Regarding claim 16, Stallings discloses a communication device (networking device with IPSec, p. 164, Fig. 6.1) connectable to a communication system (network, p. 164, Fig. 6.1) comprising a communication interface receiving a communication message (IPSec message; the interface is inherent as data is transmitted over the network in p. 164, Fig. 6.1) from a sending device (user system with IPSec, p. 164, Fig. 6.1) connected to said communication system (computers on the right send messages to/from servers on the left, Fig. 6.5), said communication message comprising a first header information (IP header, p. 175, Fig. 6.6(c), IPv4) being related with a device-type associated commitment (IP header includes version number supported, p. 197, §IPV4), said device-type associated commitment being a commitment for devices of a particular

device-type regarding what capability the devices support (support for IPv4, p. 197, §IPv4), said communication message further comprising a second header information (authentication header, p. 175, Fig. 6.6(c)) in turn comprising a first signature (MAC is calculated over immutable header fields, p. 173, §Integrity Check Value, ¶3+, which include the version) and authenticating circuitry (networking device; as authentication is performed, p. 169, #3, it is inherent that the networking device includes circuitry arranged to verify the signature) arranged to verify said first signature (authentication header authenticates the inner IP packet, p. 169, #3, p. 171, ¶1 & destination processes headers, p. 180, #3).

Regarding claim 21, Stallings discloses wherein said communication device is a server (networking device, p. 164, Fig. 6.1).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims 1-2, 4-8, 12-13, 15-16, 19 & 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over “Generic Content Download Over The Air Specification, Version 1.0” by **OMA** in view of SSL, as described by **Stallings**.

Regarding claim 1, OMA discloses providing in a first device (client, p. 24, §5.6.1) connected to a communication system (p. 12, Fig. 1), first header information (User-Agent header, p. 35, §HTTP Request for Download Descriptor) of a communication message (HTTP

Art Unit: 2134

request, p. 35, §HTTP Request for Download Descriptor), said first header information being related with a device-type associated commitment (CoolPhone/1.4), said device-type associated commitment being a commitment for devices of a particular type (CoolPhone, version 1.4) regarding what capability the devices support (version 1.4, User-Agent header, p. 35, §HTTP Request for Download Descriptor) and communicating said communication message (request) to a second device (server that responds, p. 35, §HTTP Request for Download Descriptor) connected to said communication system (p. 12, Fig. 1). OMA lacks tamper-resistantly creating a first signature in said first device based on at least tamper-resistant device-type specific information of said first device, providing, in said first device, second header information of said communication message comprising said signature and authenticating said first header information by verifying said first signature after said communicating step. However, Stallings teaches SSL, where HTTP messages are secured (p. 207, ¶1), by applying a MAC (message authentication code), encrypting, adding a header and transmitting the resulting segment and where the receiver decrypts and verifies the data (p. 208, §SSL Record Protocol). Note that in the MAC, a shared key is used (p. 209, ¶2). Therefore, since the MAC and encryption are done over the whole data, Stallings discloses tamper-resistantly (using a MAC) creating a first signature (MAC) in said first device (sender), providing, in said first device, second header information (appended header (MAC, see p. 209, Fig. 7.3, 4th segment from the top) of said communication message comprising said signature and authenticating said first header (header of original application data, such as HTTP, p. 209, Fig. 7.3, first segment) by verifying said first signature (MAC) after said communication step. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify OMA to secure the

OMA HTTP request message and as such to include the steps of tamper-resistantly creating a first signature in said first device based on at least tamper-resistant device-type specific information of said first device, providing, in said first device, second header information of said communication message comprising said signature and authenticating said first header information by verifying said first signature after said communicating step. Note that the signature is based on tamper-resistant device-type specific information of said first device (User-Agent information) in the combination. One of ordinary skill would have been motivated to perform this modification to add confidentiality and message integrity to the request data, as taught by Stallings. Note also that §5.2.1 of OMA suggests the usage of HTTPS (SSL over HTTP).

Regarding claim 2, OMA, as modified above, discloses wherein said communication system is based on HTTP (§5.2.4).

Regarding claim 4, OMA, as modified above, discloses wherein said first device is a user terminal (mobile device, p. 10, §4.1).

Regarding claim 5, OMA, as modified above, discloses wherein the second device is a server (server responds, p. 35, §HTTP Request for Download Descriptor).

Regarding claim 6, OMA, as modified above, discloses wherein said device-specific information comprises a definition of an algorithm according to which said signature is to be created (MAC algorithm is used to create the MAC, Stallings p. 209, ¶2).

Regarding claim 7, OMA, as modified above, discloses wherein said device-type specific information (User-Agent information, i.e. CoolPhone/1.4) comprises a data string being unique

for each particular device type (CoolPhone/1.4 is unique to this device, p. 35, §HTTP Request for Download Descriptor).

Regarding claim 8, OMA, as modified above, discloses wherein said step of creating a signature is additionally based on at least one item in the group of time, date and header information (based on application data, Stallings, p. 209, which, as modified, includes OMA's HTTP packet, including header, p. 35, §HTTP Request for Download Descriptor).

Regarding claim 12, OMA discloses header generation circuitry (client/mobile device, p. 24, §5.6.1 & p. 10, §4.1) configured to provide first header information (User-Agent header, p. 35, §HTTP Request for Download Descriptor) of a communication message (HTTP request, p. 35, §HTTP Request for Download Descriptor), said first header information being related with a device-type associated commitment (CoolPhone/1.4), said device-type associated commitment being a commitment for devices of a particular type (CoolPhone, version 1.4) regarding what capability the devices support (version 1.4, User-Agent header, p. 35, §HTTP Request for Download Descriptor), storage of device-type specific information (User-Agent information, p. 35, §HTTP Request for Download Descriptor) and communications circuitry (client/mobile device, p. 24, §5.6.1 & p. 10, §4.1) configured to communicate said communication message to another device (server that responds, p. 35, §HTTP Request for Download Descriptor) connected to said communication system (p. 12, Fig. 1). OMA lacks a tamper-resistant storage of device-type specific information, a tamper-resistant signature generator, arranged to create a first signature based on at least said device-type specific information and wherein the header generation circuitry is configured to provide second header information of said communication message comprising said signature. However, Stallings teaches SSL, where HTTP messages are

Art Unit: 2134

secured (p. 207, ¶1), by applying a MAC (message authentication code), encrypting, adding a header and transmitting the resulting segment and where the receiver decrypts and verifies the data (p. 208, §SSL Record Protocol). Note that in the MAC, a shared key is used (p. 209, ¶2). Therefore, since the MAC and encryption are done over the whole data, Stallings discloses tamper-resistantly (using a MAC) creating a first signature (MAC) in said first device (sender), providing, in said first device, second header information (appended header (MAC, see p. 209, Fig. 7.3, 4th segment from the top) of said communication message comprising said signature and authenticating said first header (header of original application data, such as HTTP, p. 209, Fig. 7.3, first segment) by verifying said first signature (MAC) after said communication step. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify OMA's client device to include tamper-resistant storage of device-type specific information (at least temporarily stored User-Agent information tamper-resistantly stored in MAC form, created during SSL), a tamper-resistant signature (MAC) generator, arranged to create a first signature based on at least said device-type specific information (MAC created from all of HTTP packet, including header, which includes User-Agent header) and wherein the header generation circuitry is configured to provide second header information (p. 209, Fig. 7.3, 4th segment down) of said communication message comprising said signature (append the MAC, p. 209). One of ordinary skill would have been motivated to perform this modification to add confidentiality and message integrity to the request data, as taught by Stallings. Note also that §5.2.1 of OMA suggests the usage of HTTPS (SSL over HTTP).

Regarding claim 13, OMA, as modified above, discloses wherein said communication system is based on HTTP (§5.2.4).

Regarding claim 15, OMA, as modified above, discloses wherein said first device is a user terminal (mobile device, p. 10, §4.1).

Regarding claim 16, OMA discloses a communication interface (server, p. 10, §4.2 & p. 12, Fig. 1) for receiving a communication message (HTTP request, p. 35, §HTTP Request for Download Descriptor) from a sending device (client/mobile device, p. 24, §5.6.1 & p. 10, §4.1) connected to a communication system (p. 12, Fig. 1), said communication message comprising first header information (User-Agent, p. 35, §HTTP Request for Download Descriptor) being related with a device-type associated commitment (CoolPhone/1.4), said device-type associated commitment being a commitment for devices of a particular type (CoolPhone, version 1.4) regarding what capability the devices support (version 1.4, User-Agent header, p. 35, §HTTP Request for Download Descriptor). OMA lacks the communication message further comprising second header information in turn comprising a first signature and authenticating circuitry arranged to verify said first signature. However, Stallings teaches SSL, where HTTP messages are secured (p. 207, ¶1), by applying a MAC (message authentication code), encrypting, adding a header and transmitting the resulting segment and where the receiver decrypts and verifies the data (p. 208, §SSL Record Protocol). Note that in the MAC, a shared key is used (p. 209, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify OMA's server to receive a communication message further including a second header (Stallings's appended MAC, p. 209, Fig. 7.3) comprising a first signature (MAC) and to include authenticating circuitry arranged to verify said first signature

(MAC). One of ordinary skill would have been motivated to perform this modification to add confidentiality and message integrity to the request data, as taught by Stallings. Note also that §5.2.1 of OMA suggests the usage of HTTPS (SSL over HTTP).

Regarding claim 19, OMA, as modified above, discloses wherein said communication system is based on HTTP (§5.2.4).

Regarding claim 21, OMA, as modified above, discloses wherein said communication device is a server (p. 35, §HTTP Request for Download Descriptor).

13. Claims 3, 14 & 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **OMA** and **Stallings**, as applied to claims 2, 13 & 19 above, in further view of U.S. Patent Application Publication 2006/0150257 to Leung et al. (**Leung**).

Regarding claims 3, 14 & 20, OMA, as modified, lacks wherein the device-type associated commitment is a commitment to follow Digital Rights Management compliance. However, Leung teaches that (in a DRM system), when requesting access to content, a client formulates and sends a request including a version number of the black box (core) of the DRM system (¶125). This allows the issuing server to check the version number of the black box to determine if the version is current and complies with the DRM (¶¶136-137). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify OMA, as modified above, such that the device-type associated commitment (CoolPhone/1.4) is a commitment to follow Digital Rights Management compliance. One of ordinary skill in the art would have been motivated to perform such a modification to determine if the device can be trusted with DRM content, as taught by Leung.

Allowable Subject Matter

14. Claims 9-11 & 17-18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. The following is a statement of reasons for the indication of allowable subject matter:

a. Regarding claim 9, Stallings discloses a well known concept of signature creation and verification where the authentication header contains a signature on the IP header to be verified, thus assuring integrity. However, the prior art of record fails to teach or disclose, either alone or in combination, determining a device-type of said first device based on said first header information, creating a second signature in said second device based on at least tamper-resistant information associated with said determined device-type and accepting said determined device-type as authentic if said first and second signatures agree, in combination with the other elements of the claim.

b. Regarding claim 10, Stallings discloses end-to-end communication. U.S. Patent Application Publication 2004/0054779 to Takeshima is cited for teaching a signature verification server (§133). However, since Stallings' end-to-end communication must decrypt and determine integrity for trust reasons, forwarding the data would result in less security and hence would not be applicable to SSL or IPSec. Therefore, the prior art of record fails to teach or disclose, either alone or in combination, forwarding information about said first header information and said first signature from said second device to a third device, requesting a verification of the authenticity of said first header information

by said third device and accepting said first header information as authentic if said third device provides a positive verification, in combination with the other elements of the claim. Claim 11 is objected to based on its dependence upon claim 10.

c. Regarding claim 17, Stallings (as discussed above) discloses creating a first signature based on at least device-type specific information (headers, including version, and key, see HMAC), providing a second header information (authentication header) of a communication message (IPSec message) comprising the signature and communicating the communication message to another device. However, the signature in Stallings is checked based only on the received header (verifies that the IP header, etc. has not been modified in transit). Therefore, the prior art of record fails to teach or disclose, either alone or in combination, retrieving device-type specific information corresponding to a device type determined based on said first header information and creating a second signature based on said retrieved device-type specific information and accepting the determined device-type as authentic if said first and second signatures agree, in combination with the other elements of the claim.

d. Regarding claim 18, Stallings discloses end-to-end communication. U.S. Patent Application Publication 2004/0054779 to Takeshima is cited for teaching a signature verification server (§133). However, since Stalling's end-to-end communication must decrypt and determine integrity for trust reasons, forwarding the data would result in less security and hence would not be applicable to SSL or IPSec. Therefore, the prior art of record fails to teach or disclose, either alone or in combination, forwarding information about said first header information and said first signature to a further device, requesting

a verification of the authenticity of said first header information by said further device and accepting said first header information as authentic if said further device provides a positive verification, in combination with the other elements of the claim.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

e. The Wireless Application Protocol Forum reference is cited for teaching delivering capability and preference profiles in HTTP message headers (see at least p. 72).

f. U.S. Patent Application Publication 2004/0054779 to Takeshima is cited for teaching a signature verification server (§133).

g. The Ohto reference is cited for teaching exchanging capabilities over HTTP.

h. The OMA DRM reference is cited for teaching a DRM element of a header.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

April 30, 2008

/Michael J Simitoski/

Primary Examiner, Art Unit 2134